AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

One LG Rebel 2 cellphone with serial number 709CQNL208791

Case No. MJ18-355

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The Subject Digital Media as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 2251(a)	Production of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SPECIAL AGENT CAO TRIET (DAN) HUYNH, HSI
Printed name and title

Sworn to before me pursuant to CrimRule 4.1.

Date: 08/06/2018

Judge's signature

City and state: SEATTLE, WASHINGTON

BRIAN A. TSUCHIDA, CHIEF U.S. MAGISTRATE JUDGE
Printed name and title

2018R00736

ATTACHMENT A

SUBJECT'S DIGITAL MEDIA

One LG Rebel 2 cell phone with serial number 709CQNL208791. The phone has a cracked screen and is black with a grey back cover. The cell phone was detained by HSI Seattle on July 24, 2018, from CHRISTOPHER LEE WOOD and is currently located in the secure office of HSI Seattle, 1000 Second Avenue, Suite 2300, Seattle, Washington 98104.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including photographic form and electrical, electronic, and magnetic form that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), including but not limited to:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct in any format or media.

2. Letters, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer.

3. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct.

4. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography.

5. Any and all address books, names, lists of names, telephone numbers, and addresses of minors.

6. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors.

7. Evidence of who used, owned or controlled the digital devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history.

8. Evidence of malware that would allow others to control the digital devices such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

9. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence, and/or evidence that any of the digital devices were attached to any other digital device(s).

10. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device.

11. Evidence of times the digital device(s) was used.

12. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

13. Records of Internet Protocol (IP) addresses used.

14. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

AFFIDAVIT

STATE OF WASHINGTON | ss

COUNTY OF KING

I, CAO TRIET (DAN) HUYNH, being duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Special Agent in Charge (SAC), Seattle, Washington. I have been an agent with HSI since April 2010. HSI is responsible for enforcing the customs and immigration laws and federal criminal statutes of the United States. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

2. I am a graduate of the Federal Law Enforcement Training Center (FLETC), ICE Special Agent Training Program, and have received further specialized training in investigating child pornography and child exploitation crimes. I have also had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have participated in the execution of previous search warrants, which involved child exploitation and/or child pornography offenses, and the search and seizure of computers, related peripherals, and computer media equipment. I am a member of the Seattle Internet Crimes Against Children Task Force, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children. Before joining HSI, I worked for the City of Port Townsend, Washington, Police Department as a police officer and detective for approximately nine years.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

3. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the following item belonging to CHRISTOPHER LEE WOOD:

a. One LG Rebel 2 cell phone (with cracked screen) with serial number 709CQNL208791.The item to be searched (at times referred to as the "SUBJECT'S DIGITAL MEDIA"), more fully described in Attachment A to this Affidavit, is currently located in the secure office of the HSI Seattle, 1000 Second Avenue, Suite 2300, Seattle, Washington 98104.

4. The facts set forth in this Affidavit are based on the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience.

5. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a warrant to search the property described in Attachment A for the evidence described in Attachment B, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), will be found in the SUBJECT'S DIGITAL MEDIA.

This Affidavit is being presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

INITIAL INVESTIGATION BY SEATTLE POLICE DEPARTMENT

6. On or about March 19, 2018, Seattle Police Department (SPD) Internet Crimes Against Children Detective (Det.) Danial Conine opened an investigation into a peer-to-peer (P2P) child pornography suspect within the general jurisdiction of

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Washington State. Det. Conine chose the IP address of 73.239.93.53 because he had 31 automated contraband (child pornography) connections between the dates of September 13, 2017, and February 6, 2018, resulting in over 1,400 completed downloads.

7. As part of the investigation into IP address 73.239.93.53, Det. Conine downloaded contraband files of child sexual exploitation material from a device at IP address 73.239.93.53 on or about January 23, 2018, between approximately 1410 hours and 1420 hours UTC (-0800). Det. Conine reviewed the downloaded files and described two as follows:

> 004640.jpg 7NVBEFMFBY44G34INR5ICROQOAIQTBYW: This color image depicts a prepubescent girl, approximately 9 to 11 years of age, laying down on what appears to be a bed with blue bedding. The child's age is based upon her lack of breast and pubic development, and overall body size. The child is completely naked and her left arm is raised about her head. The child's chest and vagina are both visible, and the child's waist is turned toward the camera, causing the focus of the image to be on her vagina. Also depicted in the image are two adult males, depicted nude near the bed. Both adults have erect penises, and the adult closest to the child is holding his penis with both hands.
>
> 004642.jpg WAXPX4MDOXSENTABVRBY47PCNB5TO42J: This color image depicts a prepubescent girl, approximately 4 to 6 years of age, in a bedroom setting with three other individuals. The child is kneeling on a brown pillow and holding herself up off the bed with her hands. The child is depicted nude and since her body is turned away from the camera, only her buttocks is visible, though her lack of breast development is obvious, as is the child's overall size. Also depicted in the image is an adult male, depicted nude, kneeling on the bed behind the child. The adult is holding the child's waist with his left hand and his erect penis is inserted between the child's legs, near her vagina. Depicted in the image to the left of the adult and child, is another female, approximately 12 to 14 years old. This additional female is also nude and her developing breasts are depicted. The female is holding a phallic shaped object in her right hand. The last person depicted in the image, is of unknown gender and age. This person is depicted to the right of the adult and child, and only their right leg and hands are visible. This person is holding a green lamp toward the adult and child.

8. Det. Conine believed these files depict the sexual exploitation of a minor as defined in RCW 9.68A. I have also reviewed these files and believe these files depict minors engaged in sexually explicit conduct.

9. On or about March 23, 2018, at approximately 1540 hours, Det. Conine contacted King County Superior Court Judge Sean P. O'Donnell and obtained a search

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

warrant for Comcast Communications subscriber information for IP Address 73.239.93.53.

10. On or about March 28, 2018, Det. Conine received a response from Comcast Communications that identified a residence located on 51st Avenue West, Mountlake Terrace WA connected to the subscriber of IP Address 73.239.93.53. Detective Conine confirmed via the Department of Licensing that the subscriber of IP address 73.239.93.53 resided in a home with three other individuals; one of whom was CHRISTOPHER LEE WOOD.

HSI INVESTIGATION, SEARCH WARRANT, AND ARREST

11. After confirming the address location and residents, I conducted surveillance on the residence and observed CHRISTOPHER LEE WOOD's aluminum/silver 2005 Hyundai car parked in front of the residence on May 24, 2018, and May 25, 2018. I conducted open source social media checks of all persons listed by DOL residing at the residence.

12. On or about May 31, 2018, Homeland Security Investigations (HSI) Agents including myself with assistance from other agencies executed a King County Superior Court Search Warrant on the residence located on 51st Avenue West, Mountlake Terrace, WA. Located at the residence were three individuals including CHRISTOPHER LEE WOOD and CHRISTOPHER LEE WOOD's [redacted] (minor victim # 1, MV1).

13. Seattle Police Detective (SPD) Det. Mark Misiorek and I conducted a recorded interview of CHRISTOPHER LEE WOOD following an advisement of his constitutional rights, which CHRISTOPHER LEE WOOD waived and agreed to speak with us.

14. CHRISTOPHER LEE WOOD provided information on the digital devices in the residence and provided some passwords to several devices, this included a Gateway Desktop Computer recovered from a "side room" located on the south side of the residence, a HP laptop located in CHRISTOPHER LEE WOOD'S room, and various

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

electronic storage media located in a locked safe under CHRISTOPHER LEE WOOD's bed.

15. CHRISTOPHER LEE WOOD reported that MV1 stays with him two days a week and sleeps in the same room on a top bunk while he sleeps on the lower bunk. CHRISTOPHER LEE WOOD reported his online activities included reading the news, going on YouTube, etc. CHRISTOPHER LEE WOOD requested an attorney shortly after we inquired if he downloaded videos or music and the interview was terminated.

16. During an onsite forensic preview of CHRISTOPHER LEE WOOD's digital media pursuant to the search warrant, HSI Computer Forensics Agents located numerous child pornography images on CHRISTOPHER LEE WOOD's Gateway Computer and a 16GB PNY thumb drive that was locked inside the safe underneath CHRISTOPHER LEE WOOD's bed. CHRISTOPHER LEE WOOD's Gateway computer contained the following file:

> This color image depicts a white prepubescent female with long brown hair that appears to be tied into a ponytail. This child victim (CV) is on her hands and knees on a brown sofa and nude only wearing yellow/green socks. She is positioned where her genitals and buttocks are exposed towards the camera. The CV is looking back towards the camera and has her lips puckered appearing to make a kissing gesture. There are some stuff animals visible towards the couch and to the left of the CV. The CV appears under the age of 10 as she lacks pubic or body hair, appears small in stature, and has a youthful face in appearance.

17. The following is a description of an image of child pornography found on CHRISTOPHER LEE WOOD's 16GB PNY thumb drive:

> This color image depicts a white prepubescent female with long brown hair. The child victim (CV) is lying back on a grey sofa and is fully nude. Her legs are spread and knees up exposing her genitals towards the camera. The CV has her left hand across her abdomen area. She is looking towards the camera and has her tongue sticking out. The CV appears under the age of 12 as she lacks breast development, lacks pubic or body hair, and is small in stature. Her face has a youthful appearance. Behind the CV there appears to be a desk with a monitor and a chair with a yellow square pillow with blue and orange square patterns on it.

18. On or about May 31, 2018, CHRISTOPHER LEE WOOD was arrested and booked into Snohomish County Jail for Possession of Depictions of Child Engaged in

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Sexually Explicit Conduct in the 2nd Degree and Dealing in Depictions of Child Engaged in Sexually Explicit Conduct in the 1st Degree.

PRELIMINARY FORENSIC EXAMINATION OF DIGITIAL DEVICES

19. On or about June 14, 2018, HSI Computer Forensics Analyst (CFA) Derek Quintanilla located approximately seven child pornography images on CHRISTOPHER LEE WOOD's IBM Travelstar hard drive that was seized from the search warrant on or about May 31, 2018, depicting MV1, who is currently only twelve-years-old. All these images have a distinctive red/orange/black/yellow/green multi-colored blanket with designs on it that was also found in CHRISTOPHER LEE WOOD's bedroom during the May 31, 2018, search warrant. A description of two images is provided below:

> (Carved_JPG_41710655.jpg): This color image depicts MV1 lying on a red/orange/black/yellow/green multi-colored blanket with designs on it. MV1 is wearing a purple tee shirt with the letters "G", "L", and "Z" visible on it. The MV1 is nude from her belly button down. MV1 has her legs spread and knees bent. MV1's genitals are fully exposed towards the camera. MV1's arms are also spread. MV1 is smiling towards the camera. MV1's genitals and anus are fully exposed. MV1 appears to be under the age of 10 due to her small stature, youthful face, and her lack of pubic or body hair.
>
> (Carved_JPG_52333991.jpg): This color image depicts MV1. MV1 is lying on and/or next to other bedding to include the red/orange/black/yellow/green multi-colored blanket with designs on it. MV1 is wearing the same purple tee shirt and is nude from her stomach down. MV1 has her legs spread apart and feet towards the air fully exposing her genitals and anus. MV1's arms appear to be up and above her head. MV1 is smiling towards the camera.

20. On or about June 14, 2018, CFA Quintanilla also located on CHRISTOPHER LEE WOOD's Gateway Computer, some of the same child pornography images that were located during the search warrant on or about May 31, 2018. Specifically, one child pornography file was saved in the following path: "Documents and Settings\Administrator\My Documents\My Pictures\vlcsnap-2016-08-13-04h02m14s214.png".

21. CHRISTOPHER LEE WOOD's Gateway Computer hard drive contained a Western Digital brand hard drive that bore a manufacture label indicating "Product of Thailand." Based upon my training and experience, I know that CHRISTOPHER LEE

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

WOOD's 16 GB PNY was manufactured outside the State of Washington. CHRISTOPHER LEE WOOD's IBM Travelstar hard drive bore a manufacture label indicating "MADE IN HUNGARY."

22. On or about June 15, 2018, I showed sanitized copies of some of the child pornography files of MV1 to include the files Carved_JPG_41710655.jpg and Carved_JPG_52333991.jpg to MV1's mother. MV1's mother positively identified MV1 in these child pornography images. MV1's mother reported MV1 was approximately five years old in these photographs. MV1's mother confirmed that MV1 spent the night with CHRISTOPHER LEE WOOD twice weekly for the past three to four years and that MV1 slept in the same room as CHRISTOPHER LEE WOOD when she stayed the night at his home at 51st Avenue West, Mountlake Terrace, WA. She also stated that since MV1 was four years old, CHRISTOPHER LEE WOOD would pick her up daily from school and would have her until 7PM.

23. On or about June 15, 2018, MV1 was forensically interviewed by a child forensic interviewer. MV1 was shown the child pornography images depicted of herself to include the files Carved_JPG_41710655.jpg and Carved_JPG_52333991.jpg. MV1 positively identified herself in the child pornography images but did not recall the details of the images. MV1 also believed that the child pornography images depicting her were taken in CHRISTOPHER LEE WOOD's bedroom and recognized items that belong to CHRISTOPHER LEE WOOD in the images. MV1 also recognized and remembered owning some of the clothing she was wearing in some of the images.

24. On or about June 18, 2018, I obtained an arrest warrant via a criminal complaint for CHRISTOPHER LEE WOOD from the Honorable James P. Donohue, US Magistrate Judge of the U.S. District Court for the Western District of Washington in Seattle, WA. The offenses for the arrest warrant were for violations of title 18, U.S.C. § 2251(a), (e) (Production of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography).

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

25. On or about July 24, 2018, at approximately 0207 hours, King County, WA Sheriff's Office Deputies Johnson and Lyons were dispatched to Tinkham Road and Forest Service Road 5510 in the North Bend, WA area for a disabled motorist needing a jump-start. The deputies arrived and located CHRISTOPHER LEE WOOD and his vehicle. After record checks of the vehicle and CHRISTOPHER LEE WOOD, the deputies learned that CHRISTOPHER LEE WOOD had the outstanding arrest warrant on this case. The deputies arrested him and booked him into the King County Jail in Seattle, WA.

26. During CHRISTOPHER LEE WOOD's arrest, he had a LG Rebel 2 cell phone (SUBJECT'S DIGITAL MEDIA) on his person. The SUBJECT'S DIGITAL MEDIA has a label on the back from LG stating, "MADE IN CHINA."

27. On or about July 24, 2018, at approximately 1050 hours HSI SA Curtis Crowder and I arrived at the King County Jail and took custody of CHRISTOPHER LEE WOOD and his possessions. That included the SUBJECT'S DIGITAL MEDIA, a black wallet, two sets of keys, a blue flashlight, a NFL Seahawks cap, a black belt, $5 cash, and a paper showing property CHRISTOPHER LEE WOOD had and signed for. SA Curtis and I transported CHRISTOPHER LEE WOOD to the U.S. District Courthouse in Tacoma, WA, and turned him over to the custody of the U.S. Marshals Service. The U.S. Marshals Service took possession of CHRISTOPHER LEE WOOD'S $5 cash and his current Washington State Driver's License.

TECHINCAL BACKGROUND

28. I know, based on my training and experience, that cellular phones (referred to herein generally as "smart phones") have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smart phone on their person; recent

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

investigations in this District have resulted in the discovery of child pornography files on smart phones which were carried on an individual's person at the time the phones were seized.

29. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers and computer technology have revolutionized the way in which child pornography is collected, distributed, and produced. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these images was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership based/subscription based websites to conduct business, allowing them to remain relatively anonymous.

30. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that the development of computers has also revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child pornography.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

31. Producers of child pornography can now produce both still and moving images directly from the average video or digital camera. These still and/or moving images are then uploaded from the camera to the computer, either by attaching the camera to the computer through a USB cable or similar device, or by ejecting the camera memory card from the camera and inserting it into a card reader. Once uploaded to the computer, the images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to those by which a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. Producers of child pornography can also use a scanner to transfer printed photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

32. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers, including ISPs, allow email service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet. Having said that, however, this application does not seek to reach any host computers. This application seeks permission only to search the SUBJECT'S DIGITAL MEDIA.

33. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography, and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick,

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the distributor's/recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the distributor/recipient.

34. The computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as a "hard drive") used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 1 terabyte are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage elsewhere. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

35. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in child pornography:

a. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who receive and attempt to receive child pornography may collect sexually explicit or suggestive materials in a variety of media, including

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. Those who receive and attempt to receive child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years.

d. Likewise, those who receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

e. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

36. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored information on any of a variety of computers, computer systems, digital devices, and other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another.

37. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases the items set forth in Attachment B may take the form of files, documents, and other data that is user-generated and found on a digital device. In other cases, these items may take the form of other types of data - including in some cases data generated automatically by the devices themselves.

38. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe that for the SUBJECT'S DIGITAL MEDIA, there is probable cause to believe that the items set forth in Attachment B will be stored in those digital devices for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices - in particular, a computer's internal hard drive - contain electronic evidence of how a digital device has been used, what is has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information - and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. HSI agents in this case have consulted on computer forensic matters with law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

39. Peer to Peer (P2P) file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to setup file(s)

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

and/or folder(s) on his computer so that the files can be shared with others running compatible P2P software. In essence, a user can distribute child pornography by placing child pornography in a designated shared file or folder on his computer and allowing his computer to be searched and accessed by other users of the P2P network. If, for example, Individual 1 finds a file of interest shared on Individual 2's computer, the P2P software that Individuals 1 and 2 have installed allows Individual 1 to download the file from Individual 2's computer. BitTorrent, as mentioned above in this investigation is a common P2P file sharing network. Additionally, the BitTorrent network is well known among the law enforcement community for being commonly used by collectors of child pornography.

40. The BitTorrent network can be accessed by peer computers via many different BitTorrent network clients (software or apps), examples of which include the BitTorrent client, uTorrent clientb and Vuze client, among others. These clients are publically available and typically are free P2P software programs that can be downloaded from the Internet. In normal P2P operations, as users download files or pieces of files from other peers on the BitTorrent network, other peers on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files. A person who has all the pieces of a file is termed a "seeder."

41. Files or sets of files are shared on the BitTorrent network via the use of "Torrents." A torrent is typically a small file that describes the file(s) to be shared. It is important to note that torrent files do not contain the actual file(s) to be shared, but information about the file(s) to be shared needed to accomplish a download. This information includes things such as the name(s) of the file(s) being referenced in the torrent, how many pieces make up the torrent and the "info hash" of the torrent. The "info hash" is a Secure Hash Algorithm, commonly abbreviated as SHA-1, which

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

describes the data of the file(s) referenced in the torrent. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA-1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA-1 signatures provide a certainty exceeding 99.99% that two or more files with the same SHA-1 signature are identical copies of the same file regardless of their file names. This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each torrent uniquely identifies the torrent file on the BitTorrent network. The torrent file may also contain information on how to locate file(s) referenced in the torrent by identifying "Trackers." Trackers are computers on the BitTorrent network that collate information about the peers that have recently reported they are sharing the file(s) referenced in the torrent file. A tracker is only a pointer to peers on the network who may be sharing part or all of the file(s) referenced in the torrent. Trackers do not actually have the file(s), but are used to facilitate the finding of other peers that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of tracker(s) on the BitTorrent network are not always necessary to locate peers that have file(s) being shared from a particular torrent file. There are many publically available servers on the Internet that provide BitTorrent tracker services.

42. The term "pieces" as used above refers to how many data sets are needed to complete the total download of a given torrent. The number of pieces is determined by a BitTorrent client at the time the torrent is created. A torrent may have one piece or it may have thousands of pieces. A torrent is broken up into pieces as it speeds up the ability of the network to deliver the contents of the torrent from multiple users on the

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

network. The more pieces that are available, the faster a user can obtain all the contents of a torrent file.

43. In order to locate torrent files of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include isohhunt.com and piratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate torrent files that describe the files they are looking to download. Torrent indexing websites do not host the content (files) described by torrent files, only the torrent files themselves. Once a torrent file is located on the website that meets a user's keyword search criteria, the user will download the torrent file to their computer. The BitTorrent client on the user's computer will then process that torrent file in order to find trackers or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the torrent file. It is again important to note that the actual file(s) referenced in the torrent are actually obtained directly from other peers on the BitTorrent network and not the trackers themselves. Typically, the trackers on the network return information about remote peers that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), referenced in the torrent, to include the remote peer's Internet Protocol (IP) addresses.

44. A person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website. Based on the results of the keyword search, the user would then select a torrent of interest for them to download to their computer from the website. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the BitTorrent client on the user's computer or designated external storage

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

media. The downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.

SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

45. In accordance with the information in this affidavit, law enforcement personnel will execute the search of the SUBJECT'S DIGITAL MEDIA, pursuant to this warrant, as follows:

a. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will extract data and produce a forensic copy of the SUBJECT'S DIGITAL MEDIA which may contain data or items that fall within the scope of Attachment B of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include the investigative agent(s), may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

b. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit.

CONCLUSION

46. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are located in the SUBJECT'S DIGITAL MEDIA, as more fully described in Attachment A to this Affidavit. I therefore request that the court issue a warrant authorizing a search of

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

the SUBJECT'S DIGITAL MEDIA for the item more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

CAO TRIET (DAN) HUYNH,
Affiant, Special Agent
Department of Homeland Security
Homeland Security Investigations

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on 6th day of August, 2018.

BRIAN A. TSUCHIDA
Chief United States Magistrate Judge

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

ATTACHMENT A

SUBJECT'S DIGITAL MEDIA

One LG Rebel 2 cell phone with serial number 709CQNL208791. The phone has a cracked screen and is black with a grey back cover. The cell phone was detained by HSI Seattle on July 24, 2018, from CHRISTOPHER LEE WOOD and is currently located in the secure office of HSI Seattle, 1000 Second Avenue, Suite 2300, Seattle, Washington 98104.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including photographic form and electrical, electronic, and magnetic form that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), including but not limited to:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct in any format or media.

2. Letters, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer.

3. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct.

4. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography.

5. Any and all address books, names, lists of names, telephone numbers, and addresses of minors.

6. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors.

7. Evidence of who used, owned or controlled the digital devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history.

8. Evidence of malware that would allow others to control the digital devices such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

9. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence, and/or evidence that any of the digital devices were attached to any other digital device(s).

10. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device.

11. Evidence of times the digital device(s) was used.

12. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

13. Records of Internet Protocol (IP) addresses used.

14. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970